UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/749,913	12/29/2003	Jaroslaw Sydir	Intel-013PUS	1409

7590 12/26/2007

Daly, Crowley & Mofford, LLP
c/o PortfolioIP
P.O. Box 52050
Minneapolis, MN 55402

EXAMINER	
YOUNG, NICOLE M	

ART UNIT	PAPER NUMBER
2139	

MAIL DATE	DELIVERY MODE
12/26/2007	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	Application No.	Applicant(s)	
	10/749,913	SYDIR ET AL.	
	Examiner	Art Unit	
	Nicole M. Young	2139	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *01 November 2007*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1,3-20,22-25,27-32,34 and 35* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☐ Claim(s) *1,3-20,22-25,27-32,34 and 35* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *21 March 2007* is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

A request for continued examination under 37 CFR 1.114, including the fee set forth in 37 CFR 1.17(e), was filed in this application after final rejection. Since this application is eligible for continued examination under 37 CFR 1.114, and the fee set forth in 37 CFR 1.17(e) has been timely paid, the finality of the previous Office action has been withdrawn pursuant to 37 CFR 1.114. Applicant's submission filed on November 1, 2007 has been entered.

Claims 1, 3-20, 22-25, 27-32, 34 and 35 are pending. Claims 2, 21, 26, and 33 are cancelled. Claim 35 is new.

Claim Rejections - 35 USC § 112

The 112 rejections have been overcome and are withdrawn.

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

Claims 1, 4-6, 8-20, 23-25, and 27-32 are rejected under 35 U.S.C. 103(a) as being unpatentable over **Ohta et al. (US 2002/0083317)** herein Ohta, and further in view of **Tardo (US 7,082,534)**.

Claims 1, 10, 13, 14, 15, 16, 18, 19, 20, 25, 32 disclose (Currently Amended) a processor, comprising:

a crypto unit comprising:

a cipher core configured to cipher data received; (Ohta Figure 12 and associated text show a plurality of cipher cores (303a and 303b) and a plurality of authentication buffers (304a and 304b))

a plurality of processing contexts each configured to process at least one data packet at a time and to store cipher keys and algorithm context associated with processing the at least one data packet (Paragraph [0012] teaches plural cipher processing units and paragraph [0046] teaches different cipher algorithms used to encrypt/decrypt the data. This would correspond to the "plurality of processing contexts");

Ohta teaches authentication cores configured to authenticate the ciphered data in Figure 12, Authentication Processing Unit 305a and 305b and associated text in paragraph [0104] Ohta does not teach but Tardo teaches, at least two authentication cores each implementing a different authentication algorithm as shown in Figures 2 and 3 and explained in column 4 lines 48-67 through column 5 lines 1-36. Figure 2 shows 2

authentication engines MD5 225 and SHA1 227. Figure 3 and associated text teach choosing the authentication engine based on the encryption as in column 5 lines 25-29. It would be obvious to one of ordinary skill in the art at the time of invention to use 2 different authentication algorithms of Tardo in two different authentication cores of Ohta. The motivation to combine would be that in paragraph [0046] of Ohta it states that the authentication algorithm includes HMAC-MD5-96 and HMAC-SHA-1-96. Therefore, as shown in Ohta the authentication cores include different algorithms); and

an authentication buffer configured to store the ciphered data and provide the ciphered data to the authentication cores each in an amount based on the corresponding authentication algorithm implemented. (Ohta Figure 12, Data Accumulation Unit 304a and 304b; paragraph [0011] states "a data block accumulation unit that outputs the accumulated amount to the authentication processing unit when it reaches the smallest data block size for the authentication processing")

wherein the authentication buffer comprises a number of buffer elements corresponding to a number of processing contexts (Figure 12 shows two buffers and two authentication processing units).

Claims 4, 23, 28 disclose (Currently Amended) the processor according to claim 1, wherein each of the buffer elements stores data for a respective one of the processing contexts (Figure 12 and associated text show a corresponding number of data block accumulation units to encryption processing units).

Claim 5 discloses (Currently Amended) the network processor according to claim 4, wherein the buffer elements have a size that is at least as large as a largest authentication algorithm block size implemented by the authentication cores (Ohta Figure 12, Data Accumulation Unit 304a and 304b; paragraph [0011] states "a data block accumulation unit that outputs the accumulated amount to the authentication processing unit when it reaches the smallest data block size for the authentication processing").

Claim 6 discloses (Currently Amended) the processor according to claim 1, wherein the crypto unit further comprises a plurality of cipher cores, and a plurality of authentication buffer elements (Figure 12 and associated text show a plurality of cipher cores (303a and 303b) and a plurality of authentication buffers (304a and 304b)).

Claim 8 discloses (Currently Amended) the processor according to claim 6, wherein one of the authentication cores processes data in 16-byte blocks and another one of the authentication cores processes data in 64-byte blocks. (The rejection of claim one above and also, paragraph [0016] teaches outputting blocks of data to the encryption and authentication processors in multiples of 8 bits, which would include all processor blocks in claims 8 and 9.)

Claim 9 discloses (Currently Amended) the network processor according to claim 8, wherein one of the cipher core cores processes data in 8-byte blocks and another one

of the cipher cores processes data in and/or 16-byte blocks. (The rejection of claim one above and also, paragraph [0016] teaches outputting blocks of data to the encryption and authentication processors in multiples of 8 bits, which would include all processor blocks in claims 8 and 9.)

Claim 11 discloses the method according to claim 10, further comprising ciphering data received in a first one of a plurality of cipher cores to form the ciphered data (Figure 12 and associated text show a plurality of cipher cores (303a and 303b) and a plurality of authentication buffers (304a and 304b).

Claim 12 discloses (Currently Amended) the method according to claim 10, further comprising ciphering data received using a first one of a plurality of cipher algorithms to form the ciphered data (Tardo Figure 2, DES 221 and AES 223).

Claims 17, 30, 31 disclose (Currently Amended) the method according to claim 10, further comprising determining whether data is to be ciphered (Ohta paragraph [0046], processing contexts).

Claims 24, 29 discloses (Original) the device according to claim 20, wherein the device includes one or more of a router, network switch, security gateway, storage area network client, and server (Paragraph [0089] teaches a router, firewall, and security

gate connecting plural computers. This is equivalent to the hardware devices mentioned in claims 20, 24, and 29).

Claim 7 is rejected under 35 U.S.C. 103(a) as being unpatentable over **Ohta et al. (US 2002/0083317)** and **Tardo (US 7,082,534)**, and further in view of **Corder (US 7,069,447).**

Ohta and Tardo teach claims 1 and 6 of the current application which claim 7 depends from as shown above. It however, does not teach a connection using a multiplexer device. Ohta teaches connections using a data path connection switching unit as in paragraph [0013].

Corder teaches authentication and encryption buffers and units connected with a multiplexer in column 7 lines 1-21.

In Ohta paragraph [0129] it teaches that the data path connection switching unit is used to provide various paths flexibly combined to fully take advantage of the multiple units. Therefore it would be obvious to one of ordinary skill in the art at the time of invention that this same inherent property of a multiplexer would be an alternate choice.

Claims 3, 22, 27, 34, and 35 are rejected under 35 U.S.C. 103(a) as being unpatentable over **Ohta et al. (US 2002/0083317)** and **Tardo (US 7,082,534)**, and further in view of **Yoaz et al. (6,697,932)** herein referred to as Yoaz.

Claims 3, 22, 27, 34, and 35 disclose (Currently Amended) the processor according to claim 1, wherein the plurality of processing contexts (Ohta Figure 12 and associated text show a corresponding number of data block accumulation units to encryption processing units).

Ohta does not teach processing contexts are configured to allow latency of loading cryptographic key material and packet data to be hidden by pipelining loading of the packet data and the key material into a first portion of the plurality of processing contexts with processing of the packet data in a second portion of the plurality of processing contexts.

Yoaz teaches processing contexts are configured to allow latency of loading cryptographic key material and packet data to be hidden by pipelining loading of the packet data and the key material into a first portion of the plurality of processing contexts with processing of the packet data in a second portion of the plurality of processing contexts (column 3 lines 57-67).

It would be obvious to one of ordinary skill in the art at the time of invention was made to use pipelining to hide the latency of data within the Ohta system, since Yoaz states at column 3 lines 57-67 "this invention minimizes the stall time caused by waiting for missing data" for example the authentication buffer in Ohta.

Response to Arguments

Applicant's arguments filed November 1 2007 have been fully considered but they are not persuasive.

Applicant states that Ohta does not disclose processing contexts as disclosed in claim one. The Examiner respectfully disagrees. The Applicants statements refer to the prior objection of application 10/749,913. As shown above, The Examiner interprets the processing contexts to be processing units 303a, 303b, 305a and 305b. Ohta states in paragraph [0105] that the processing units output the data block by block while encrypting and authenticating. The Examiner has further clarified the rejection based on Ohta.

Conclusion

The prior art made of record and not relied upon is considered pertinent to applicant's disclosure.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Nicole M. Young whose telephone number is 571-270-1382. The examiner can normally be reached on Monday through Friday, alt Fri off, 8:00am-5:30pm.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ayaz Sheikh can be reached on 571-272-3795. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

NMY
12/19/2007

AYAZ SHEIKH
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100